UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/743,302	03/08/2001	Jan-Erik Ekberg	NC18017	8257

26933 7590 01/07/2004

ROBERT C. ROLNIK
NOKIA INC.
6000 CONNECTION DRIVE
MD 1-4-755
IRVING, TX 75039

EXAMINER	
LE, DUY K	

ART UNIT	PAPER NUMBER
2685	

DATE MAILED: 01/07/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/743,302	EKBERG, JAN-ERIK	
	Examiner	Art Unit	
	Duy K Le	2685	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-22 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-22 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 6.
4) ☐ Interview Summary (PTO-413) Paper No(s). _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-3, 6-9, 11-13, 15-17, and 19-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 6,061,346 to Nordman in view of He et al. (U.S. Patent 6,088,451).

As to claim 1, the Nordman reference discloses authentication method for telecommunications networks, especially for IP networks, in accordance with which method the identity of a subscriber attached to the network is authenticated ("a method, and associated apparatus, for accessing a private IP network with a wireless host by way of a wireless access network. Once authenticated and permitted access to the private IP network, the wireless host becomes a virtual host of the private IP network" (Abstract, lines 1-5)),

characterized by

- in a network terminal (TE1) 16 (Figure 1), using a subscriber identity module (SIM) 18 essentially of the same kind as in a known mobile communications system (MN), which identity module is such that a response is obtained as a result of a challenge given to it as input ("the radio communication station 10 includes a radio transceiver, here a GSM mobile terminal 16. The mobile terminal 16 includes a SIM (Subscriber Identity Module) card 18" (Col. 5, line 66 to

Col. 6, line 2). "The SIM card 18 includes a storage location 24 for storing authentication information" (Col. 6, lines 4-5)),

- using a special security server (SS) 76 (Figure 1) in the network so that when a terminal attaches to the network, a message of a new user is transmitted to the security server ("the HLR 76 includes an authentication center (not separately shown) at which, inter alia, an IMSI (International Mobile Subscriber Identity) and a value of a pseudo-random number are stored" (Col. 6, lines 56-59). "Appropriate commands are generated at the wireless host to initiate a request for access to the private IP network 14" (Col. 7, lines 28-30). "The mobile terminal 16 generates a request over the air interface as an uplink signal 56 communicated to the BTS 52. In a GSM communication system, an attach procedure is initiated. The BTS 52 forwards the request through the BSC 62 to the MSC/VLR 66. The IMSI and pseudo-random number of values are retrieved from the HLR 76 and an authentication procedure is carried out" (Col. 7, lines 32-39). "The authentication procedure authenticates, i.e., confirms that the mobile terminal 16 is permitted to communicate by way of the network infrastructure forming the wireless access network" (Col. 7, lines 42-45)),

However, the Nordman reference does not expressly disclose fetching subscriber authentication information corresponding to the said new user from the said mobile communications system to the said network which authentication information contains at least a challenge and a response, and performing the authentication based on the authentication information obtained from the mobile communications system by transmitting the said challenge to the terminal through the network, by generating a response from the challenge in the identity

module of the terminal and by comparing the response with the response received from the mobile communications system.

The He reference teaches fetching subscriber authentication information corresponding to the said new user from the said mobile communications system to the said network, which authentication information contains at least a challenge and a response, and performing the authentication based on the authentication information obtained from the mobile communications system by transmitting the said challenge to the terminal through the network, by generating a response from the challenge in the identity module of the terminal and by comparing the response with the response received from the mobile communications system (See "the authentication process", Col. 17, line 53 to Col. 18, line 32).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the method of Nordman to be characterized by fetching subscriber authentication information corresponding to the said new user from the said mobile communications system to the said network, which authentication information contains at least a challenge and a response, and performing the authentication based on the authentication information obtained from the mobile communications system by transmitting the said challenge to the terminal through the network, by generating a response from the challenge in the identity module of the terminal and by comparing the response with the response received from the mobile communications system. One would have been motivated to make such a modification in view of the suggestion in He to control access to the network and protect network resources and information.

As to claim 2, as cited in claim 1, Nordman-He discloses method as defined in claim 1, characterized in that fetching of the subscriber's authentication information from the mobile communications system is started from the security server (SS) in response to the said message (See "the authentication process", Col. 17, line 53 to Col. 18, line 32 in He).

As to claims 3 and 17, as cited in claim 1, Nordman-He discloses method as defined in claims 1 and 16. The He reference further discloses that in response to a successful authentication, registration of the subscriber is performed as a client of a separate key management system ("user identification and registration will be centrally administered and managed at the site of the authentication server 202" (Col. 16, lines 39-41). "The authentication server 202 can maintain a database of records for the user accounts in the registration database 210" (Col. 16, lines 50-52)).

As to claim 6, Nordman-He discloses method as defined in claim 1. The Nordman reference further discloses that the subscriber's authentication information is fetched with the aid of a separate proxy server (HP) 82 (Figure 1), which functions as a network element emulating the visitor location register VLR of the mobile communications system and which requests the authentication information from an authentication centre AuC 76 located in connection with the subscriber's home location register HLR 76 in the same way as the mobile communications system's own visitor location register ("the HLR 76 includes an authentication center (not separately shown) at which, inter alia, an IMSI (International Mobile Subscriber Identity) and a value of a pseudo-random number are stored" (Col. 6, lines 56-59). "Both the BSC 62 and HLR 76 are further coupled to a SGSN (Serving GPRS Support Node) 82. The SGSN 82 is further coupled to the backbone network 46 by way of lines 88. Therefore, the SGSN 82 is coupled to

the private IP network 14" (Col. 7, lines 1-7). "The mobile terminal 16 generates an attach request to attach to the wireless access network formed of the network infrastructure of the GSM system" (Col. 8, lines 50-52). "During the attach procedure, the values of the IMSI, the WHI, and other associated subscriber data is downloaded from the HLR 76 to the appropriate one of the MSC/VLR 66 and SGSN 82" (Col. 8, lines 57-60)).

As to claim 7, Nordman-He discloses method as defined in claim 1. The Nordman reference further discloses that the subscriber's authentication information is fetched with the aid of a separate proxy server (BP) 82 (Figure 1), which functions as a network element emulating the mobile communications system's base station controller and which is in connection with the mobile communications system's mobile switching centre (MSC) 66 for fetching the authentication information from an authentication centre AuC 76 located in connection with the subscriber's home location register HLR 76 in the same way as the authentication information is fetched to the mobile communications system's own base station controller ("the HLR 76 includes an authentication center (not separately shown) at which, inter alia, an IMSI (International Mobile Subscriber Identity) and a value of a pseudo-random number are stored" (Col. 6, lines 56-59). "Both the BSC 62 and HLR 76 are further coupled to a SGSN (Serving GPRS Support Node) 82. The SGSN 82 is further coupled to the backbone network 46 by way of lines 88. Therefore, the SGSN 82 is coupled to the private IP network 14" (Col. 7, lines 1-7). "The mobile terminal 16 generates an attach request to attach to the wireless access network formed of the network infrastructure of the GSM system" (Col. 8, lines 50-52). "During the attach procedure, the values of the IMSI, the WHI, and other associated subscriber data is downloaded from the HLR 76 to the appropriate one of the MSC/VLR 66 and SGSN 82" (Col. 8,

lines 57-60). "The mobile terminal 16 generates a "PDP routing context activation request" to the SGSN 82 or an access to the MSC/VLR 66" (Col. 9, lines 1-3). "Pursuant to the activation request to the SGSN 82 or the access to the MSC/VLR 66, an indication of which HIPN is to be accessed is further provided to the SGSN or MSC/VLR" (Col. 9, lines 9-12). "The appropriate one of the SGSN 82 and the MSC/VLR 66 analyzes the value of the IMSI provided thereto and determines the address of the default, private IP network" (Col. 9, lines 20-22)).

As to claim 8, Figure 1 in Nordman discloses authentication system for telecommunications networks, especially for IP networks, which system includes authentication means for authenticating the identity of a subscriber who has attached to the network ("a method, and associated apparatus, for accessing a private IP network with a wireless host by way of a wireless access network. Once authenticated and permitted access to the private IP network, the wireless host becomes a virtual host of the private IP network" (Abstract, lines 1-5)),

characterized in that the authentication means include

- a subscriber identity module (SIM) 18 connected to the network's terminal (TE1) 16, the module being essentially similar to the subscriber identity module used in a separate mobile communications system (MN), whereby a response can be determined from a challenge given to the identity module as input ("the radio communication station 10 includes a radio transceiver, here a GSM mobile terminal 16. The mobile terminal 16 includes a SIM (Subscriber Identity Module) card 18" (Col. 5, line 66 to Col. 6, line 2). "The SIM card 18 includes a storage location 24 for storing authentication information" (Col. 6, lines 4-5)),

- messaging means (HA) 56 for sending a message when a terminal attaches to the network ("the mobile terminal 16 generates a request over the air interface as an uplink signal 56

communicated to the BTS 52. In a GSM communication system, an attach procedure is initiated" (Col. 7, lines 32-35)),

- a special security server (SS) 76 for receiving the said message,

However, the Nordman reference does not disclose

- means for requesting authentication information corresponding to a subscriber from the said mobile communications system (MN), which information contains at least a challenge and a response, and

- on the side of the said network, data transmission and checking means for transmitting the challenge through the network to the identity module, for returning the response from the terminal to the network and for comparing the received response with the response received from the mobile communications system.

The He reference teaches means for requesting authentication information corresponding to a subscriber from the said mobile communications system (MN), which information contains at least a challenge and a response, and on the side of the said network, data transmission and checking means for transmitting the challenge through the network to the identity module, for returning the response from the terminal to the network and for comparing the received response with the response received from the mobile communications system (See "the authentication process", Col. 17, line 53 to Col. 18, line 32).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the method of Nordman to be characterized in that the authentication means include means for requesting authentication information corresponding to a subscriber from the said mobile communications system (MN), which information contains at

least a challenge and a response, and on the side of the said network, data transmission and checking means for transmitting the challenge through the network to the identity module, for returning the response from the terminal to the network and for comparing the received response with the response received from the mobile communications system. One would have been motivated to make such a modification in view of the suggestion in He to provide means to control access to the network and protect network resources and information.

As to claims 9 and 20, Nordman-He discloses system as defined in claims 8 and 19, characterized in that the said identity module is the subscriber identity module (SIM) used in the GSM network ("the radio communication station 10 includes a radio transceiver, here a GSM mobile terminal 16. The mobile terminal 16 includes a SIM (Subscriber Identity Module) card 18" (Col. 5, line 66 to Col. 6, line 2). "The SIM card 18 includes a storage location 24 for storing authentication information" (Col. 6, lines 4-5); Nordman).

As to claim 11, Nordman-He discloses system as defined in claim 8. The Nordman reference discloses the means for requesting authentication information include the said security server 76 (Figure 1) and a proxy server (HP, BP) 82, which is connected to the GSM network ("the HLR 76 includes an authentication center (not separately shown) at which, inter alia, an IMSI (International Mobile Subscriber Identity) and a value of a pseudo-random number are stored" (Col. 6, lines 56-59). "Both the BSC 62 and HLR 76 are further coupled to a SGSN (Serving GPRS Support Node) 82. The SGSN 82 is further coupled to the backbone network 46 by way of lines 88. Therefore, the SGSN 82 is coupled to the private IP network 14" (Col. 7, lines 1-7)).

As to claim 12, Nordman-He discloses system as defined in claim 11. The Nordman reference discloses that the proxy server functions as a network element emulating the visitor location register VLR of the GSM network ("the mobile terminal 16 generates an attach request to attach to the wireless access network formed of the network infrastructure of the GSM system" (Col. 8, lines 50-52). "During the attach procedure, the values of the IMSI, the WHI, and other associated subscriber data is downloaded from the HLR 76 to the appropriate one of the MSC/VLR 66 and SGSN 82" (Col. 8, lines 57-60). "The mobile terminal 16 generates a "PDP routing context activation request" to the SGSN 82 or an access to the MSC/VLR 66" (Col. 9, lines 1-3). "Pursuant to the activation request to the SGSN 82 or the access to the MSC/VLR 66, an indication of which HIPN is to be accessed is further provided to the SGSN or MSC/VLR" (Col. 9, lines 9-12). "The appropriate one of the SGSN 82 and the MSC/VLR 66 analyzes the value of the IMSI provided thereto and determines the address of the default, private IP network" (Col. 9, lines 20-22)).

As to claim 13, Nordman-He discloses system as defined in claim 11. The Nordman reference discloses that the proxy server functions as a network element emulating the base station controller BSC of the GSM network ("the mobile terminal 16 generates an attach request to attach to the wireless access network formed of the network infrastructure of the GSM system" (Col. 8, lines 50-52). "During the attach procedure, the values of the IMSI, the WHI, and other associated subscriber data is downloaded from the HLR 76 to the appropriate one of the MSC/VLR 66 and SGSN 82" (Col. 8, lines 57-60). "The mobile terminal 16 generates a "PDP routing context activation request" to the SGSN 82 or an access to the MSC/VLR 66" (Col. 9, lines 1-3). "Pursuant to the activation request to the SGSN 82 or the access to the

MSC/VLR 66, an indication of which HIPN is to be accessed is further provided to the SGSN or MSC/VLR" (Col. 9, lines 9-12). "The appropriate one of the SGSN 82 and the MSC/VLR 66 analyzes the value of the IMSI provided thereto and determines the address of the default, private IP network" (Col. 9, lines 20-22)).

As to claim 15, the Nordman reference discloses authentication method for telecommunications networks, especially for IP networks, in accordance with which method the identity of a subscriber attached to the network is authenticated ("a method, and associated apparatus, for accessing a private IP network with a wireless host by way of a wireless access network. Once authenticated and permitted access to the private IP network, the wireless host becomes a virtual host of the private IP network" (Abstract, lines 1-5)),

characterized by

- in a network terminal (TE1) 16 (Figure 1), using a subscriber identity module (SIM) 18 essentially similar to the one used in a known mobile communications system (MN), which identity module is such that a response is obtained as a result of a challenge given to it as input ("the radio communication station 10 includes a radio transceiver, here a GSM mobile terminal 16. The mobile terminal 16 includes a SIM (Subscriber Identity Module) card 18" (Col. 5, line 66 to Col. 6, line 2). "The SIM card 18 includes a storage location 24 for storing authentication information" (Col. 6, lines 4-5)),

- storing subscriber-specific authentication information in a database (DB), the information being in that way essentially similar to the information used for authentication in the said mobile communications system that it contains at least a challenge and a response ("the HLR 76 includes an authentication center (not separately shown) at which, inter alia, an IMSI

(International Mobile Subscriber Identity) and a value of a pseudo-random number are stored" (Col. 6, lines 56-59). "The IMSI and pseudo-random number of values are retrieved from the HLR 76 and an authentication procedure is carried out" (Col. 7, lines 37-39)),

- using a special security server (SS) 76 (Figure 1) in the network so that when a terminal attaches to the network, a message about the new user is transmitted to the security server ("Appropriate commands are generated at the wireless host to initiate a request for access to the private IP network 14" (Col. 7, lines 28-30). "The mobile terminal 16 generates a request over the air interface as an uplink signal 56 communicated to the BTS 52. In a GSM communication system, an attach procedure is initiated. The BTS 52 forwards the request through the BSC 62 to the MSC/VLR 66. The IMSI and pseudo-random number of values are retrieved from the HLR 76 and an authentication procedure is carried out" (Col. 7, lines 32-39)),

- in response to the message, retrieving authentication information of the subscriber corresponding to the new user from the said database (DB) ("The mobile terminal 16 generates a request over the air interface as an uplink signal 56 communicated to the BTS 52. In a GSM communication system, an attach procedure is initiated. The BTS 52 forwards the request through the BSC 62 to the MSC/VLR 66. The IMSI and pseudo-random number of values are retrieved from the HLR 76 and an authentication procedure is carried out" (Col. 7, lines 32-39)).

However, the Nordman reference does not disclose performing authentication based on the authentication information obtained from the database by transmitting the said challenge through the network to the terminal, by generating a response from the challenge in the identity module of the terminal and by comparing the response with the response obtained from the database. The He reference teaches performing authentication based on the authentication

information obtained from the database by transmitting the said challenge through the network to the terminal, by generating a response from the challenge in the identity module of the terminal and by comparing the response with the response obtained from the database (See "the authentication process", Col. 17, line 53 to Col. 18, line 32).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the method of Nordman to be characterized by performing authentication based on the authentication information obtained from the database by transmitting the said challenge through the network to the terminal, by generating a response from the challenge in the identity module of the terminal and by comparing the response with the response obtained from the database. One would have been motivated to make such a modification in view of the suggestion in He to control access to the network and protect network resources and information.

As to claim 16, Nordman-He discloses method as defined in claim 15. The Norman reference discloses that the database is stored in connection with the security server ("the HLR 76 includes an authentication center (not separately shown) at which, inter alia, an IMSI (International Mobile Subscriber Identity) and a value of a pseudo-random number are stored" (Col. 6, lines 56-59)).

As to claim 19, Figure 1 in Nordman discloses authentication system for telecommunications networks, especially for IP networks, which system includes authentication means for authentication of the identity of a subscriber attached to the network ("a method, and associated apparatus, for accessing a private IP network with a wireless host by way of a wireless

access network. Once authenticated and permitted access to the private IP network, the wireless host becomes a virtual host of the private IP network" (Abstract, lines 1-5)),

characterized in that the authentication means include

- a subscriber identity module (SIM) 18, which is connected to a network terminal (TE1) 16 and which is essentially similar to the subscriber identity module used in a separate mobile communications system (MN), whereby a response can be determined from the challenge given as input to the identity module ("the radio communication station 10 includes a radio transceiver, here a GSM mobile terminal 16. The mobile terminal 16 includes a SIM (Subscriber Identity Module) card 18" (Col. 5, line 66 to Col. 6, line 2). "The SIM card 18 includes a storage location 24 for storing authentication information" (Col. 6, lines 4-5)),

- messaging means (HA) 56 for sending a message when a terminal attaches to the network ("the mobile terminal 16 generates a request over the air interface as an uplink signal 56 communicated to the BTS 52. In a GSM communication system, an attach procedure is initiated" (Col. 7, lines 32-35)),

- a special security server (SS) 76 for receiving the said message,

- database means (SS, DB) 76, which include a database (DB), wherein subscriber specific authentication information is stored, which is in such a way essentially similar to the information used for authentication in the said mobile communications system that it includes at least a challenge and a response, and retrieval means (SS) for retrieving subscriber specific authentication information from the said database in response to the message ("the HLR 76 includes an authentication center (not separately shown) at which, inter alia, an IMSI (International Mobile Subscriber Identity) and a value of a pseudo-random number are stored"

(Col. 6, lines 56-59). "Appropriate commands are generated at the wireless host to initiate a request for access to the private IP network 14" (Col. 7, lines 28-30). "The mobile terminal 16 generates a request over the air interface as an uplink signal 56 communicated to the BTS 52. In a GSM communication system, an attach procedure is initiated. The BTS 52 forwards the request through the BSC 62 to the MSC/VLR 66. The IMSI and pseudo-random number of values are retrieved from the HLR 76 and an authentication procedure is carried out" (Col. 7, lines 32-39)),

However, the Nordman reference does not disclose that on the side of the said network, data transmission and checking means for transmitting the said challenge through the network to the identity module, for returning the response from the terminal to the network and for comparing the received response with the response received from the database. The He reference teaches on the side of the said network, data transmission and checking means for transmitting the challenge through the network to the identity module, for returning the response from the terminal to the network and for comparing the received response with the response received from the database (See "the authentication process", Col. 17, line 53 to Col. 18, line 32).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the system of Nordman to be characterized in that the authentication means include on the side of the said network, data transmission and checking means for transmitting the challenge through the network to the identity module, for returning the response from the terminal to the network and for comparing the received response with the response received from the mobile communications system. One would have been motivated to make such a modification in view of the suggestion in He to provide means to control access to the network and protect network resources and information.

3. Claims 4-5, 14, 18, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 6,061,346 to Nordman in view of He et al. (U.S. Patent 6,088,451) and further in view of Campbell (U.S. Patent 6,148,402).

As to claims 4 and 18, Nordman-He discloses method as defined in claims 3 and 17. However, it does not disclose that the known Kerberos system is used as the key management system. The Campbell reference discloses "illustrated in FIG. 2 is a block diagram of the client server system utilizing the Kerberos security system of the prior art" (Col. 4, lines 64-66). "As part of the login sequence and before prompted for the password, the message 24 is sent across the network to the Kerberos authentication security server 13" (Col. 5, lines 5-7). "Then, the authentication security server 13 looks up the user login name and the service name in the Kerberos database and obtains an encryption key for each" (Col. 5, lines 13-15).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the method of Nordman-He to be characterized in that the known Kerberos system is used as the key management system, as taught by Campbell, in order to provide system security based on a well-known and standardized authentication system.

As to claim 5, Nordman-He-Campbell discloses method as defined in claim 4. The Campbell reference further teaches that the subscriber-specific authentication information obtained from the mobile communications system also includes a key (Kc), whereby the subscriber is registered as a client of the Kerberos system so that the key is registered (a) as the client's password and (b) as a password for a service formed for the client's IP address or for a subscriber identity (IMSI) used in the mobile communications system ("the encryption keys used by the Kerberos are one-way encrypted passwords similar to what is stored in the password entry

field of a normal unix password file. The authentication security server 13 forms a response 44 back to the client login program on the workstation. This response contains a ticket that grants the user access to the requested ticket is the core of the Kerberos system" (Col. 5, lines 14-23). "The messages and the ticket is encrypted using the client's encryption key and encryption password which is contained in the Kerberos database on security server 13 in the service authentication module 42" (Col. 5, lines 25-28). See also Col. 5, lines 29 to Col. 6, line 18).

As to claims 14 and 22, Norman-He discloses system as defined in claims 11 and 19. However, it does not disclose that that the system further includes a Kerberos server (KS) which is known as such and as the user of which the subscriber will be registered as a result of a successful authentication.

The Campbell reference teaches that the system further includes a Kerberos server (KS) which is known as such and as the user of which the subscriber will be registered as a result of a successful authentication ("illustrated in FIG. 2 is a block diagram of the client server system utilizing the Kerberos security system of the prior art" (Col. 4, lines 64-66). "As part of the login sequence and before prompted for the password, the message 24 is sent across the network to the Kerberos authentication security server 13" (Col. 5, lines 5-7). "Then, the authentication security server 13 looks up the user login name and the service name in the Kerberos database and obtains an encryption key for each" (Col. 5, lines 13-15). "The authentication security server 13 forms a response 44 back to the client login program on the workstation. This response contains a ticket that grants the user access to the requested server 12." (Col. 5, lines 18-22)).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the method of Nordman-He to be characterized in that the

system further includes a Kerberos server (KS) which is known as such and as the user of which the subscriber will be registered as a result of a successful authentication, as taught by Campbell, in order to provide system security based on a well-known and standardized authentication system.

4. Claims 10 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 6,061,346 to Nordman in view of He et al. (U.S. Patent 6,088,451) and further in view of Yuan (U.S. Patent 6,496,704).

As to claims 10 and 21, Nordman-He discloses system as defined in claims 8 and 19. However, it does not disclose that the messaging means are adapted into a home agent (HA) in accordance with the mobile IP network. The Yuan reference teaches the messaging means are adapted into a home agent (HA) in accordance with the mobile IP network ("the Mobile IP uses the home agent 70 and the foreign agent 82 route packets to/from the mobile host 74" (Col. 4, lines 7-9). "The home agent 70 is responsible for intercepting the IP packets destined for the mobile host 74 and for forwarding the IP packets to the foreign agent 82 of the mobile host 74" (Col. 4, lines 11-14)).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the system of Nordman-He to be characterized in that the messaging means are adapted into a home agent (HA) in accordance with the mobile IP network, as taught by Yuan, in order to route packets to/from a mobile host between different networks.

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Ahvenainen (U.S. Patent 6,148,192) discloses checking the access right of a subscriber equipment.

b. Salin (U.S. Patent 5,625,671) discloses method of checking the identity of a subscriber equipment.

c. Geiselman et al. (U.S. Patent 6,466,780) discloses method and apparatus for securing digital communications.

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Duy K Le whose telephone number is 703-305-5660. The examiner can normally be reached on 8:30 am - 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edward F Urban can be reached on 703-305-4385. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Duy Le
November 12, 2003

EDWARD F. URBAN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600